White Hat Wi-Fi

by dual_parallel
http://www.oldskoolphreak.com

Questions. A vice that is enjoying an insecure technology will lead to many. Wi-fi, 802.11b specifically, is oh so alluring to explore. And if you're familiar at all with the technology, you know that you can literally stumble upon a network and discover new things.

And with new discovery come ethical questions; questions of how far to take exploration and what to do if that exploration leads to knowledge of insecurities. I'll talk about such questions in this article, as well as a little technology.

Nothing's better than a good decaf mocha and free wi-fi. I frequent a locally-owned chain of cafes for just such pleasures. Like all of you, I like a little exploration with my mocha. Visiting with my Linux laptop and Orinoco Gold, I su-minused and typed 'ifconfig'.

```
eth0      Link encap:Ethernet  HWaddr 00:02:2D:XX:XX:XX
          inet addr:192.168.254.42 Bcast:192.168.254.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:7139 (6.9 Kb)  TX bytes:6570 (6.4 Kb)
          Interrupt:3 Base address:0x100

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:784 (784.0 b)  TX bytes:784 (784.0 b)
```

Knowing the range of IPs that the WAP was handing out, I fired up nmap to see what was around.

```
# nmap -sS -O 192.168.254.* | tee nmap.txt
```

There were some results that were a little surprising...

Interesting ports on 192.168.254.254:

```
(The 1655 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
Device type: broadband router
Running: FlowPoint embedded, ASCOM embedded, SpeedStream embedded
OS details: FlowPoint/2000 - 2200 SDSL Router (v1.2.3 - 3.0.4) or ASCOM
Timeplex Access Router, DSL Router: Flowpoint 144/22XX v3.0.8 or
SpeedStream 5851 v4.0.5.1
```

Telnet open on the router? Eighty open for browser-based administration I could see.